UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/844,448	04/27/2001	Gregory Neil Houston	05456.105005	9082

7590 11/17/2006

W. Scott Petty, Esq.
KING & SPALDING
45th Floor
191 Peachtree Street, N.E.
Atlanta, GA 30303

EXAMINER	
SON, LINH L D	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 11/17/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/844,448	HOUSTON ET AL.	
	Examiner	Art Unit	
	Linh LD Son	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 August 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-59* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-59* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. **This Office Action is responding to the Amendment received on 08/21/06.**

2. **Claims 1-59 are pending.**

Response to Arguments

3. **Applicant's arguments filed 08/21/06 have been fully considered but they are not persuasive.**

4. **As** per remark on page 19, Applicant argues that "*Hill reference fails to teach generating security event data comprising a plurality of alerts with a plurality of security devices at a first location in response to detecting a security event in a distributed computing environment, and providing one or more variables operable for analyzing and filtering the security event data*".

Examiner respectfully traverses the application's argument. After further search and consideration of the amended claims, Examiner determines that Hill still teaches the amended claim language above. Hill discloses a method of collecting security event types from the plurality of security agents at an event manager (SOM Processor 40). The event manager (SOM processor 40) simulates the collected security events to generate the security event data (simulated attacks). The simulated attack constitutes several security event types. The event manger (SOM processor 40) trains simulated

attacks to create signatures to filtering and analyzing security events at the security agents. Therefore, Hill still teaches the amended limitation.

Similar reject basis is applied to the rest of the amended independent claims. See the rejection below.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 27-29, and 31-32 are rejected under 35 U.S.C. 102(e) as being anticipated by Hill et al, US Patent No. 6088804, hereinafter "Hill" (Cited in PTO 892 01/22/03).

7. As per claim 27:

Hill discloses "A computer-implemented system for managing security event data collected from a plurality of security devices (Fig 1) comprising:

a plurality of security devices operable for generating security event data (e.g. simulated attack) comprising a plurality of alerts (e.g. security event types) that are

generated in response to detecting a security event in a distributed computing environment; " in (Col 4 lines 53-55, and Col 5 lines 320-35 and lines 52-55);

> **Data about security events is collected by security agents 36 and transmitted via links 28, links 32, and a communication link 38 to a processor 40.**
>
> **For purposes of this description, an attack is defined as a plurality of security events 50 occurring substantially concurrently in a given sampling period at a plurality of nodes 24 (FIG. 1). The sampling period is an arbitrary amount of time that is of a sufficient length to receive enough security events to form an attack signature (discussed below) for an attack.**
>
> A simulated attack includes at least one of security event types 56, but more realistically **a simulated attack constitutes several security event types 56 as illustrated in first simulated attack 55.**

"an event manager (SOM Processor 40) coupled to the security devices, the even manager operable for collecting security event data from the security devices and analyzing the security event data with scope criteria (signature) comprising one or more definable variables operable for analyzing and filtering the security event data, the variables comprising ***at least one*** of a location of a security event , a source of security event, a destination address of the security event, **a security event type**, a priority of a security event, and an identification of a system that detected a security event," in (Col 5 line 39 to Col 6 line 20) and

> **In this example, security event types 56 include destructive virus, snooping virus, worm, Trojan horse, FTP requests, and network overload.**
>
> In addition to security event types 56 and percentage of security events 50 per event type in column 58, training signatures 53 include location identifiers 60. **Location identifiers 60 identify the nodes 24 in network 22 where security events may take place**. Location identifiers 60 are important for ascertaining an attack severity 61 for each of simulated attacks 52. Attack severity 61 is a level of security breach that one of simulated attacks 52 could cause computer network 22. The greater attack severity 61, the more damaging the security breach would be.

(34) Following task 98, a task 100 is performed by SOM processor 40 (FIG. 1). SOM processor 40 compares a vector representative of first attack signature 94 (FIG. 6) to each of training signatures 53 as mapped in display map 66 (FIG. 4).

the event manager operable for applying the scope criteria to the security event data to produce result data" in (Col 8 lines 35-47); and

(35) In response to comparing task 100, a task 102 selects one of training signatures 53 that most closely matches attack signature. With reference back to FIG. 3, the security event types 56 and frequency of security events 50 shown in column 58 of training signature 54 most closely resembles first attack 92. Those skilled in the art will recognize that other factors will contribute to the selection of a most closely resembling training signature. Other factors may include but are not limited to, the location identifiers for each of the affected nodes, network hierarchy, and so forth.

"one or more clients (Nodes 24) coupled to the event manager operable to perform an action in response to receiving analyzed security event data from the event manager and displaying the result data comprising filtered alerts based on the scope criteria" in (Col 8 lines 4-11, and Col 8 line 63 to Col 9 line 7).

(30) In response to task 82, a task 86 is performed through each of security agents 36. Task 86 causes SOM processor 40 to be notified of an outcome of the repulsing task through one of security agents 36 associated with that node 24. The notification may include data describing a security event type, a location identifier for the node 24, and whether or not the attack was successfully repulsed. Following notification task 86, program control proceeds to a task 88.

8. As per claim 28:

Hill discloses "the system of claim 27, wherein the event manager comprises a database server operable for storing the collected security event data and the analyzed security event data" in (Col 8 lines 12-19, and Col 7 lines 45-65)

9. As per claim 29:

Hill discloses the system of claim 27, wherein the event manager comprises an application server operable for creating an incident from the security event data for preparing a response (Col 8 lines 1-21).

10. As per claim 31:

Hill discloses the system of Claim 27, wherein multiple clients operable for receiving analyzed security data are coupled to the event manager (Col 8 lines 1-21).

11. As per claim 32:

Hill discloses "The method of Claim 27, wherein the action performed by the client is rendering a chart containing analyzed security event data (Figure 7).

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. Claim s 1-26, 30, and 33-59 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hill et al, US Patent No. 6088804, hereinafter "Hill" (Cited in PTO 892 01/22/03) in view of Baker, US/6775657.

14. As per claims 1, 18, 34, and 49:

Hill discloses "A method for managing security event data collected from a security devices in a distributed computing environment" in (Figure 1) "comprising the steps of:

generating security event data (e.g. attack) comprising a plurality of alerts (e.g. security event types) with a plurality of security devices at a first location (e.g. SOM Processor 40) in response to detecting a security event in a distributed computing environment;" in (Col 4 lines 53-55, and Col 5 lines 320-35 and lines 52-55);

> **Data about security events is collected by security agents 36 and transmitted via links 28, links 32, and a communication link 38 to a processor 40.**
>
> **For purposes of this description, an attack is defined as a plurality of security events 50 occurring substantially concurrently in a given sampling period at a plurality of nodes 24 (FIG. 1). The sampling period is an arbitrary amount of time that is of a sufficient length to receive enough security events to form an attack signature (discussed below) for an attack.**
>
> **A simulated attack includes at least one of security event types 56, but more realistically a simulated attack constitutes several security event types 56 as illustrated in first simulated attack 55.**

"providing ***one or more variables*** operable for analyzing and filtering the security event data, the variables ***comprising at least one of*** a location of a security event, a source of security event, a destination address of the security event, **a security**

event type, a priority of a security event, and an identification of a system that detected a security event" in (Col 5 line 39 to Col 6 line 20);

> **In this example, security event types 56 include destructive virus, snooping virus, worm, Trojan horse, FTP requests, and network overload.**
>
> In addition to security event types 56 and percentage of security events 50 per event type in column 58, training signatures 53 include location identifiers 60. **Location identifiers 60 identify the nodes 24 in network 22 where security events may take place**. Location identifiers 60 are important for ascertaining an attack severity 61 for each of simulated attacks 52. Attack severity 61 is a level of security breach that one of simulated attacks 52 could cause computer network 22. The greater attack severity 61, the more damaging the security breach would be.

"creating scope criteria (e.g. Training Signature 53) by ***selecting one or more*** (Hill teaches of training the scope criteria using the event type variable) of the variables (security event types and node identification) operable for analyzing and filtering the security event data (attack) " in (Col 5 lines 46-65, Col 5 line 65 to Col 6 line 5);

> **Training signatures 53 for simulated attacks 52 are defined by a plurality of security events 50 of at least one security event type 56 in this example.** Security events 50 are presented in database 48 in a column 58 as a percentage of security events per event type. In other words, column 58 represents the numbers of nodes 24 (FIG. 1) affected by each of security event types 56. A simulated attack includes at least one of security event types 56, but more realistically a simulated attack constitutes several security event types 56 as illustrated in first simulated attack 55. Each of security event types 56 are capable of causing an anti-security effect on computer network 22. In other words, the attacker is performing an unauthorized action on network 22. In this example, **security event types 56 include destructive virus, snooping virus, worm, Trojan horse, FTP requests, and network overload.** However, those skilled in the art will recognize that security event types may include these and/or additional evolving types of security events relative to the computer network for which dynamic network security system 20 (FIG. 1) is used.
>
> In addition to security event types 56 and percentage of security events 50 per event type in column 58, **training signatures 53 include location identifiers 60**. Location identifiers 60 identify the nodes 24 in network 22

where security events may take place. Location identifiers 60 are important for ascertaining an attack severity 61 for each of simulated attacks 52.

"collecting security event data generated by the plurality of security devices located at a first location" in (Col 4 lines 53-55);

Data about security events is collected by security agents 36 and transmitted via links 28, links 32, and a communication link 38 to a processor 40

"*storing the collected security event data at a second location* "

"analyzing and filtering the collected security event data with the scope criteria to produce result data" in (Col 8 lines 35-46);

(34) Following task 98, a task 100 is performed by S**OM processor 40 (FIG. 1). SOM processor 40 compares a vector representative of first attack signature 94 (FIG. 6) to each of training signatures 53** as mapped in display map 66 (FIG. 4).

(35) **In response to comparing task 100, a task 102 selects one of training signatures 53 that most closely matches attack signature. With reference back to FIG. 3, the security event types 56 and frequency of security events 50 shown in column 58 of training signature 54 most closely resembles first attack 92. Those skilled in the art will recognize that other factors will contribute to the selection of a most closely resembling training signature.** Other factors may include but are not limited to, the location identifiers for each of the affected nodes, network hierarchy, and so forth.

"transmitting the result data to one or more clients; and

displaying the result data comprising filtered alerts based on the scope criteria" in (Col 8 lines 4-11, and Col 8 line 63 to Col 9 line 7).

(30) In response to task 82, a task 86 is performed through each of security agents 36. **Task 86 causes SOM processor 40 to be notified of an outcome of the repulsing task through one of security agents 36 associated with that node 24. The notification may include data describing a security event type, a location identifier for the node 24, and whether or not the attack was successfully repulsed.** Following notification task 86, program control proceeds to a task 88.

However, Hill does directly teach "storing the collected security event data at a second location". Hill does teach of a security events database in Col 7 lines 40-45.

Nevertheless, Baker teaches Multilayered Intrusion Detection System and Method, which includes a method of collecting security event data and storing it in a multiple security event database for availability purpose in (Col 8 lines 45-47).

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Hill's teaching to incorporate Baker's disclosures of having security event database at different location in the network for availability purpose (Col 8 lines 45-47).

15. As per claims 2, 21, 35, and 54:

Hill discloses "The method of claims 1, 16, 34, and 49, further comprising storing one or more of the scope criteria, the security event data, and the result data in a database (Col 8 lines 12-19).

16. As per claim 3, 5, 20, 30 and 36:

Hill discloses "the method of claims 1, 16, and 27, wherein the first location is a distributed computing environment (Figure 1), the second location is a database server (Baker, Col 8 lines 45-47), and the third location is an application server (Col 5 lines 15-20) to which the plurality of clients are coupled".

17. As per claims 4, 14, 19, 38, 47, and 53:

Hill discloses "the method of claims 1, 16, 34, and 49, wherein collecting the security event data comprises generating security event data from a sensor" in (Col 4 lines 30-40);

"sending the security event data from the sensor to a collector" in (Col 8 lines 12-19); and

"converting the event data to a common format" in (Col 5 lines 37).

18. As per claims 6 and 39:

Hill discloses "the method of claims 1 and 35, further comprising searching the stored security event data for additional information identifying a security event" in (Col 5 lines 26-45).

19. As per claims 7 and 40:

Hill discloses "the method of claims 1 and 35, further comprising: polling a database server for current stored security event data;

analyzing the current stored security event data to produce current result data; and

rendering the current result data" in (Col 5 lines 26-45).

20. As per claims 8 and 41:

Hill discloses "The method of claims 1 and 34, further comprising polling for messages containing information about scope criteria, security event data, or result data (Col 5 lines 26-45).

21. As per claims 9 and 42:

Hill discloses "The method of claims 1 and 34, further comprising pushing messages to a client wherein the messages contain information about scope criteria, security event data, or result data (Col 4 lines 30-40, and Col 8 lines 4-11).

22. As per claims 10, 17, 43, and 50:

Hill discloses "The method of claims 1, 16, 34, and 49, wherein the step of rendering result data comprises presenting the result data in a chart format (Figure 7).

23. As per claims 11, 22, 44, and 55:

Hill discloses "The method of claims 1, 16, and 34, wherein in response to analyzing the collected security event data, an action is executed (Col 7 line 63 to Col 8 line 12).

24. As per claims 12, 23, 45, and 56:

Hill and Baker disclose "The method of claims 11, 22, and 44.

However, Hill does not mention the action is clearing security event data from storage.

Nevertheless, it would have been obvious at the time of the invention for one having ordinary skill in the art to realize that the capability of clearing out the data must be exist in the invention of Hill, since it is inevitable to contain unlimited data in any storage devices.

25. As per claims 13, 24, 46, and 57:

Hill discloses "The method of claims 11, 22, 44, and 55, wherein the action is creating an incident from result data for preparing a response (Col 7 line 63 to Col 8 line 12).

26. As per claims 15, 26, 48, and 59:

Hill discloses "A computer-readable medium having computer-executable instructions for performing the steps recited in claims 1, and 34" in (Col 35-45)

27. As per claim 16:

The rejection basis of claim 1 is incorporate. Further, Hill discloses applying the scope criteria to the security event data at a third location to produce a result, the result accessible by a plurality of clients coupled to a server" in (Fig 1, Col 8 lines 15-35, and Col 5 lines 45-65).

28. **As per claim 25:**

Hill discloses "the method of claim 16, further comprising applying additional scope criteria to a plurality of results" in (Col 7 lines 40-63).

29. As per claim 33:

Hill discloses "The method of Claim 1, further comprising the step of rendering the result data in a manageable format for the plurality of clients (Figure 7).

30. As per claims 37, and 51-52:

Hill discloses "The method of Claims 34, and 49, further comprising the step of creating and editing the scope criteria for filtering the security event data (Col 5 lines 1-6, and Col 5 lines 25-38).

31. As per claim 58:

Hill discloses "the method of claim 49, further comprising applying additional scope criteria to a plurality of results" in (Col 8 lines 35-47, and Col 9 lines 35-45).

Conclusion

32. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, THIS ACTION IS MADE FINAL. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

33. **Any inquiry concerning this communication or earlier communications from the examiner should be directed to Linh LD Son whose telephone number is 571-272-3856. The examiner can normally be reached on 9-6 (M-F).**

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Linh LD Son
Examiner
Art Unit 2135

HOSUK SONG
PRIMARY EXAMINER